

# Schlüsselhierarchie im VAU-Protokoll

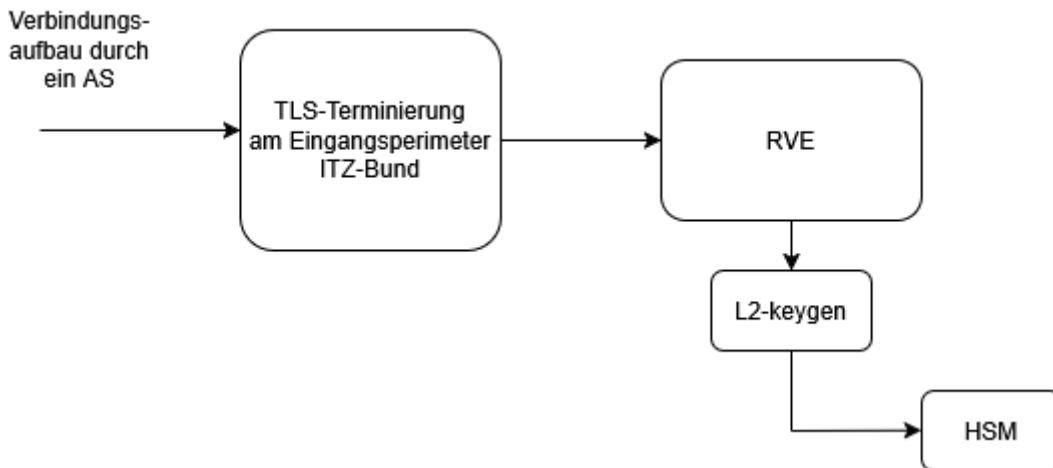
Was zum Spezial-Thema "Schlüsselhierarchie im VAU-Protokoll"

- Schlüsselhierarchie

# Schlüsselhierarchie

## Orientierungshilfe

Zur Orientierung ein Architektur-Diagramm:



RVE = "Request-Verarbeitende Einheit" = Endpunkt eines VAU-Kanals in der VST, also deutlich nach der TLS-Terminierung

## Schlüsselhierarchie in der Handshake-Phase des VAU-Protokolls

Wie in jedem nichttrivialen kryptographischen Protokoll gibt es auch im VAU-Protokoll verschiedene Schlüssel. Diese Schlüssel sind in einer Schlüsselhierarchie angeordnet. Wir betrachten einige Schlüssel aus der Handshake-Phase (VAU-Protokoll-Verbindungsaufbau) und ignorieren, der Einfachheit der Darstellung willen, auf die abgeleiteten AES/GCM-Schlüssel.

Verwendungsdauer

Ort

Ebene 1 (L1)	privater Schlüssel zu vst-cert.der (aus Komponenten-PKI TI)	max. 5 Jahre	HSM
-----------------	---	--------------	-----

---

Ebene 2 (L2)	"semistatische Schlüsselpaare ECDH und Kyber" A_24425 signiert über HSM	max. 7200 Sekunden	RVE
-----------------	---	-----------------------	-----

---

Ebene 3 (L3)	KEM-shared-secret ephemeral (ss_e) KEM-shared-secret semi-static (ss_s)	wenige Sekunden	RVE
-----------------	--	--------------------	-----

Die L2-Schlüssel haben eine flexible Gültigkeitsdauer (

[https://gemspec.gematik.de/docs/gemSpec/gemSpec\\_Krypt/latest/#A\\_24425-01](https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/#A_24425-01) ). In der PoC-Implementierung ([https://bitbucket.org/andreas\\_hallof/fdf/src/master/vst/](https://bitbucket.org/andreas_hallof/fdf/src/master/vst/) ) sind sie maximal 7260 Sekunden (2:01 h) gültig und werden alle 3600 Sekunden (1h) neu erzeugt. Im Rahmen der Erzeugung werden die öffentlichen L2-Schlüssel gemäß A\_24425-01 vom HSM mittels dessen Langzeit-Identität signiert.

Wichtig ist noch zu betonen, dass für einen passiven Angreifer (der also nicht große Teile der Infrastruktur des VST unter seiner Kontrolle hat) die Kenntnis der privaten L2-Schlüssel keinen Vorteil erzielt.